



## UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
 United States Patent and Trademark Office  
 Address: COMMISSIONER OF PATENTS AND TRADEMARKS  
 Washington, D.C. 20231  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/244,203	02/04/1999	BRETT L. HOWARD		3485

7590 11/27/2002

BLAKE CASSELS & GRAYDON LLP  
 BOX 25, COMMERCE COURT WEST  
 199 BAY STREET  
 TORONTO, ONTARIO, M5L 1A9  
 CANADA

EXAMINER	
CALLAHAN, PAUL E	
ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 11/27/2002

Please find below and/or attached an Office communication concerning this application or proceeding.

Application No.

09/244,203

Applicant(s)

HOWARD ET AL.

Examiner

Paul E. Callahan

Art Unit

2134

**Office Action Summary***-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --***Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) Responsive to communication(s) filed on 11 July 2002.
- 2a) This action is FINAL.      2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.
- 4) Claim(s) 19-33 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) Claim(s) \_\_\_\_\_ is/are allowed.
- 6) Claim(s) 19-33 is/are rejected.
- 7) Claim(s) \_\_\_\_\_ is/are objected to.
- 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Disposition of Claims**

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on \_\_\_\_\_ is/are: a) accepted or b) objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) The proposed drawing correction filed on \_\_\_\_\_ is: a) approved b) disapproved by the Examiner.  
If approved, corrected drawings are required in reply to this Office action.
- 12) The oath or declaration is objected to by the Examiner.

**Priority under 35 U.S.C. §§ 119 and 120**

- 13) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All b) Some \* c) None of:
1. Certified copies of the priority documents have been received.
  2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.
- 14) Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) The translation of the foreign language provisional application has been received.
- 15) Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)                             | 4) <input type="checkbox"/> Interview Summary (PTO-413) Paper No(s). _____  |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)         | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ | 6) <input type="checkbox"/> Other: _____                                    |

Application/Control Number: 09/244,203  
Art Unit: 2134

Page 2

**DETAILED ACTION**

1. The Applicant's request for reconsideration of the holding of abandonment in the case is valid and the holding of abandonment in the case has been rescinded. See MPEP 711.03(b). The reply received 7/12/02 is timely under 37 CFR 1.136.

*Correction to inventorship under 1.48(f) is accepted.*

2. Claims 1-18 have been cancelled without prejudice by the amendment received July 12, 2002. New claims ~~1-19~~<sup>19-33</sup> have been added by the amendment and have been examined.

***Response to Amendment***

3. The amendment filed July 11, 2002 is objected to under 35 U.S.C. 132 because it introduces new matter into the disclosure. 35 U.S.C. 132 states that no amendment shall introduce new matter into the disclosure of the invention. The added material, which is not supported by the original disclosure, is as follows: on page 25 the passage which reads "The first access port and second access port each provide mutually independent access to the memory buffer. The second bus is not connected to the first bus." The preamble to new claim 19 indicates that the new claims are directed towards a different, new invention. The new preamble indicates that the claims are drawn towards a system for ciphering data for transmission by a communications device. The preamble to original claim 1 indicated that the claims were drawn towards a system for ciphering data stored within a memory buffer. Claim 21 now recites a "message digesting module" whereas no such module carrying out a process of generation of a message digest, as it is understood as a term of art in the field of cryptography, was found in the original specification or claims in the instant application.

Applicant is required to cancel the new matter in the reply to this Office Action.

Application/Control Number: 09/244,203  
Art Unit: 2134

Page 3

***Response to Arguments***

4. Applicant's arguments filed 7/11/2002 have been fully considered but they are not persuasive.

Applicant argues that the instant invention may be distinguished from the teachings of Lorenz '201 by asserting that Lorenz does not teach separate buses as is now claimed in the instant application. However a careful reading of Lorenz will show that separate busses are taught at fig. 2 items 9 and 10.

Applicant argues that new claim 19 may be distinguished from the teachings of Lorenz by asserting that Lorenz does not teach or suggest the use of a data processor to generate ciphered data and check the ciphered data for integrity. However a signal processor containing a ciphering unit is taught in fig. 3 and comprises a signal processor as taught in fig.s 1 and 2 as discussed in col. 3 lines 52-62. Lorenz teaches checking the integrity of the data in col. 3 lines 20-25 (autocorrelation and cross correlation functions).

Applicant asserts that the Examiner failed to advance a motive to combine the features of which Official Notice was taken with the teachings of Lorenz in the rejection of claims 4, 6, 7, and 14. However a careful reading of the previous Office Action in the case will reveal that such was taught at page 5 paragraph 9 of the previous Office Action in the case. Evidence of the motive to combine may be found in the general state of knowledge in the art at the time of the invention where the use of a hashing means that comprises HMAC hashing, or encryption of communications with DES or Triple DES would increase the security of a communications system.

***Claim Rejections - 35 USC § 112***

Application/Control Number: 09/244,203  
Art Unit: 2134

Page 4

5. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

6. Claims 19-33 are rejected under 35 U.S.C. 112, first paragraph, as containing subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. New claim 19 contains new matter not found in the original set of claims or in the original specification of: the first access port and second access port each provide mutually independent access to the memory buffer, and the second bus is not connected to the first bus. Additionally, the preamble to new claim 19 indicates that the new claims are directed towards a different, new invention. The new preamble indicates that the claims are drawn towards a system for ciphering data for transmission by a communications device. The preamble to original claim 1 indicated that the claims were drawn towards a system for ciphering data stored within a memory buffer. New claim 21 now recites a "message digesting module" whereas no such module carrying out a process of generation of a message digest, as it is understood as a term of art in the field of cryptography, was found in the original specification or claims in the instant application. This new matter does not find support in the original specification in the case.

*Claim Rejections - 35 USC § 102*

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

Application/Control Number: 09/244,203  
Art Unit: 2134

Page 5

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

8. Claims 19, 21, 24, 25, 28, 31, and 32 are rejected under 35 U.S.C. 102(b) as being clearly anticipated by Lorenz et al. US Patent 5,799,201.

As per claim 19, 31, and 32, Lorenz teaches a system for ciphering data for transmission by a communication device (abstract), comprising: A memory device having a memory buffer, a first access port receiving bits of data connected to said memory buffer, and a second access port connected to said memory buffer; and a data processing processor connected to said first access port via a first bus; a ciphering processor connected to said second access port via a second bus wherein said first access port and said second access port each provide mutually independent access to said memory buffer and where data bits are stored in the memory so as to reassemble a packet of data, (fig.2 items 3a and 3b, items 4 and 5 Data Processors, items 9 and 10 Data Buffers, fig. 3 items 35 Encryptor, col. 4 lines 29-40) said second bus is not connected to said first bus (shown by fig. 2 items 9 and 10 Data Buses not connected) said data processing processor is adapted to receive said data and provide said data to said memory buffer over said first bus, said ciphering processor is adapted to receive said data from said memory buffer over said second bus (fig. 2 items 3a, 3b), generate ciphered data from said data, generate integrity check information (col. 3 lines 20-25: autocorrelation and cross correlation functions) for said ciphered data using said data and provide said ciphered data to said memory buffer over said second bus (fig. 3 items 35, 38)

As per claim 21, Lorenz teaches encryption means (fig. 3 item 35 Encryptor) and digesting means for performing verification operations (fig. 1 data processor, fig. 2 items 14, 18 ALU).

Application/Control Number: 09/244,203  
Art Unit: 2134

Page 6

As per claim 24, Lorenz teaches a memory buffer that comprises dual port RAM (col. 4 lines 4-10).

As per claims 25 and 28, Lorenz teaches a data processing processor (fig. 2 Data Processor) comprising a security module for retrieving security association data from the memory buffer (fig. 2 items 3a, 3b), for ciphering the data (fig. 3 item 35 Encryptor).

***Claim Rejections - 35 USC § 103***

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

8. Claims 20, 22, 23, 29, 30, and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lorenz et al. US Patent 5,799,201, and Official Notice taken as detailed below.

As per claims 20, 22, and 23, Lorenz does not teach a hashing means, or a hashing means comprising HMAC hashing means, or an encryption means using DES or triple-DES. Official Notice may be taken however, that such steps are old and well known in the art of processor systems utilizing the features of Lorenz and utilized to carry out encryption operations. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to have incorporated these features into the system of Lorenz. It would be advantageous to do so because use of a hashing means, or a hashing means comprising HMAC hashing, or encryption via DES or triple DES would increase the security of the system.

Application/Control Number: 09/244,203  
Art Unit: 2134

Page 7

As per claims 29 and 30, Lorenz does not teach first and second processors clocked by different clock sources that are asynchronous to one another. However official Notice may be taken that such arrangements of clock sources within processor systems carrying out encryption processing are old and well known in the art. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to have incorporated this feature into the system of Lorenz. It would have been advantageous to do so as this would increase the security of the system by making it more difficult compromise the security of the encryption processing by matching the power consumption of the processors to the encryption processing being carried out.

As per claim 33, Lorenz does not teach the communications system as part of a gateway between a private and a public network in a secure virtual private network. However Official Notice may be taken that the use of such a ciphering system in a gateway or a firewall between a private and a public network is a step that is old and well known in the art. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to have incorporated the system of Lorenz into a gateway or firewall. It would have been desirable to do so as this would increase the security of data transmitted over an insecure public network.

*Conclusion*

9. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

Application/Control Number: 09/244,203

Page 8

Art Unit: 2134

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul E. Callahan whose telephone number is (703) 305-1336.

The examiner can normally be reached on M-F from 9 to 5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, can be reached on (703) 305-1830. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 746-7239 Official Faxes, (703) 746-7240 Unofficial Faxes, and (703) 746-7238 After Final Faxes.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

11/20/02

Paul Callahan

*Gilberto Barron*  
GILBERTO BARRON  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100